What is claimed is:

1. A method of scanning a storage device for viruses, comprising:

determining physical portions of the storage device that have been modified since a previous virus scan; and

scanning at least parts of the physical portions for viruses.

2. A method, according to claim 1, wherein the physical portions correspond to tracks of the storage device.

3. A method, according to claim 1, wherein the physical portions correspond to sectors of the storage device.

4. A method, according to claim 1, wherein the physical portions correspond to subportions of the storage device.

5. A method, according to claim 1, wherein determining the physical portions of the storage device that have been modified includes:

creating a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

6. A method, according to claim 5, wherein creating the table includes copying an other table provided by the storage device.

7. A method, according to claim 5, wherein creating the table includes using an other table provided by the storage device.

8. A method of scanning a storage device for viruses, comprising:

determining physical portions of the storage device that have been modified since a previous virus scan;

mapping the portions to logical entities; and

scanning at least some of the logical entities for viruses.

9. A method, according to claim 8, wherein the physical portions correspond to tracks of the storage device.

10. A method, according to claim 8, wherein the physical portions correspond to sectors of the storage device.

11. A method, according to claim 8, wherein the physical portions correspond to subportions of the storage device.

12. A method, according to claim 8, wherein the logical entities are files.

13. A method, according to claim 8, wherein determining physical portions of the storage device that have been modified includes:

creating a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

14. A method, according to claim 8, further comprising:

prior to scanning the logical entities, selecting the logical entities according to at least one predetermined criterion.

15. A method, according to claim 14, wherein the at least one predetermined criterion is at least one of: logical entity type and date of last modification.

16. A method, according to claim 8, wherein scanning the logical entities includes scanning logical entities having one of a predetermined set of types.

17. A method, according to claim 16, wherein the predetermined types include at least one of: executable files, files that affect system configuration, Java scripts, Web based interpreted/executed files, Web pages having particular tags, and particularly identified data packets.

18. A method, according to claim 8, wherein scanning the logical entities includes scanning entities having a date of last modification that is after a most previous virus scan.

19. A method, according to claim 8, wherein scanning the logical entities includes scanning entities having one of a predetermined set of types and having a date of last modification that is after a most previous virus scan

20. A method, according to claim 8, wherein scanning the logical entities includes:

for each of the logical entities having a date of last modification that is prior to a most previous virus scan, comparing a current size value of the entity with a previous size value of the entity prior to the most previous virus scan; and

scanning entities having at least one of: a date of last modification that is after a most previous virus scan and the current size value that is different than the previous size value.

21. A method, according to claim 8, wherein scanning the logical entities includes:

for each of the logical entities having one of a predetermined set of types and having a date of last modification that is prior to a most previous virus scan, comparing a current size value of the entity with a previous size value of the entity prior to the most previous virus scan; and

scanning entities having one of the predetermined set of types and having at least one of: a date of last modification that is after a most previous virus scan and the current size value that is different than the previous size value.

22. A computer program product for scanning a storage device for viruses, comprising:

means for determining physical portions of the storage device that have been modified since a previous virus scan; and

means for scanning at least parts of the physical portions for viruses.

23. A computer program product, according to claim 22, wherein the physical portions correspond to tracks of the storage device.

24. A computer program product, according to claim 22, wherein the physical portions correspond to sectors of the storage device.

25. A computer program product according to claim 22, wherein the physical portions correspond to subportions of the storage device.

26. A computer program product, according to claim 22, wherein means for determining the physical portions of the storage device that have been modified includes:

means for creating a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

means for setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

27. A computer program product, according to claim 26, wherein means for creating the table includes means for copying an other table provided by the storage device.

28. A computer program product, according to claim 26, wherein means for creating the table includes means for using an other table provided by the storage device.

29. A computer program product for scanning a storage device for viruses, comprising:

means for determining physical portions of the storage device that have been modified since a previous virus scan;

means for mapping the portions to logical entities; and

means for scanning at least some of the logical entities for viruses.

30. A computer program product, according to claim 29, wherein the physical portions correspond to tracks of the storage device.

31. A computer program product, according to claim 29, wherein the physical portions correspond to sectors of the storage device.

32. A computer program product, according to claim 29, wherein the physical portions correspond to subportions of the storage device.

33. A computer program product, according to claim 29, wherein the logical entities are files.

34. A computer program product, according to claim 29, wherein means for determining physical portions of the storage device that have been modified includes:

means for creating a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

means for setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

35. A computer program product, according to claim 29, further comprising:

means for selecting the logical entities according to at least one predetermined criterion prior to scanning the logical entities.

36. A computer program product, according to claim 35, wherein the at least one predetermined criterion is at least one of: logical entity type and date of last modification.

37. A computer program product, according to claim 29, wherein means for scanning the logical entities includes means for scanning logical entities having one of a predetermined set of types.

38. A computer program product, according to claim 37, wherein the predetermined types include at least one of: executable files, files that affect system configuration, Java scripts, Web based interpreted/executed files, Web pages having particular tags, and particularly identified data packets.

39. A computer program product, according to claim 29, wherein means for scanning the logical entities includes scanning entities having a date of last modification that is after a most previous virus scan.

40. A computer program product, according to claim 29, wherein means for scanning the logical entities includes scanning entities having one of a predetermined set of types and having a date of last modification that is after a most previous virus scan.

41. An antivirus unit, comprising:

means for coupling to at least one storage device;

means for determining physical portions of the storage device that have been modified since a previous virus scan; and

means for scanning at least parts of the physical portions for viruses.

42. An antivirus unit, according to claim 41, wherein the physical portions correspond to tracks of the storage device.

43. An antivirus unit, according to claim 41, wherein the physical portions correspond to sectors of the storage device.

44. An antivirus unit, according to claim 41, wherein the physical portions correspond to subportions of the storage device.

45. An antivirus unit, according to claim 41, further comprising:

a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

means for setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

46. An antrivirus scanning unit, according to claim 41, wherein said means for coupling includes means for coupling to only one storage device.

47. An antivirus unit, according to claim 41, wherein said means for coupling includes means for coupling to more than one storage device.

48. An antivirus unit, according to claim 41, further comprising:

means for coupling to at least one host.

49. An antivirus unit, according to claim 48, wherein said antivirus unit is interposed between said at least one storage device and said at least one host.

50. An antivirus unit, according to claim 48, wherein said antivirus unit is implemented as a process running on the at least one host.

51. An antivirus unit, according to claim 41, wherein said antivirus unit is implemented using stand alone hardware.

52. An antivirus unit, according to claim 41, wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device.

53. An antivirus unit, comprising:

means for determining physical portions of the storage device that have been modified since a previous virus scan;

means for mapping the portions to logical entities; and

means for scanning at least some of the logical entities for viruses.

54. An antivirus unit, according to claim 53, wherein the physical portions correspond to tracks of the storage device.

55. An antivirus unit, according to claim 53, wherein the physical portions correspond to sectors of the storage device.

56. An antivirus unit, according to claim 53, wherein the physical portions correspond to subportions of the storage device.

57. An antivirus unit, according to claim 53, wherein the logical entities are files.

58. An antivirus unit, according to claim 53, further comprising:

a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

means for setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

59. An antivirus unit, according to claim 53, further comprising:

means for selecting the logical entities according to at least one predetermined criterion prior to scanning the logical entities.

60. An antivirus unit, according to claim 59, wherein the at least one predetermined criterion is at least one of: logical entity type and date of last modification.

61. An antivirus unit, according to claim 53, wherein means for scanning the logical entities scans logical entities having one of a predetermined set of types.

62. An antivirus unit, according to claim 61, wherein the predetermined types include at least one of: executable files, files that affect system configuration, Java scripts, Web based interpreted/executed files, Web pages having particular tags, and particularly identified data packets.

09715811.110700